Towards Fine-Grained and Application-Centric Access Control for Wireless Sensor Networks*

Nelson Matthys, Rehan Afzal, Christophe Huygens, Sam Michiels, and Wouter Joosen
IBBT-DistriNet, Katholieke Universiteit Leuven
B-3001, Leuven, Belgium
{firstname.lastname}@cs.kuleuven.be

Danny Hughes
Computer Science and Software Engineering
Xi'an Jiaotong-Liverpool University
215123 Suzhou, China
daniel.hughes@xjtlu.edu.cn

ABSTRACT

The emerging reality of wireless sensor networks deployed as long-lived infrastructure required to serve multiple applications necessitates the development of fine-grained security support. Specifically, to allow sensor nodes to participate in multiple concurrent applications, access control is required on a per-application basis. This paper presents a policy-driven security architecture for wireless sensor networks that addresses the concern of fine-grained access control and secure deployment of security policies, while respecting the resource-constrained nature of wireless sensor networks. A prototype of this system has been realized and evaluated using the LooCI component model and the Sun SPOT sensor network platform.

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Access controls, Authentication

General Terms

Security, Design, Performance

Keywords

Security, Component models, Policy-based Management

1. INTRODUCTION

Over the last few years, Wireless Sensor Networks (WSNs) have evolved into long-lived infrastructure on which various applications from multiple actors may be deployed. Previous work [1, 3] has showed that run-time reconfigurable component models are a good fit to deal with the dynamic, resource-constrained characteristics of WSNs, in combination with their ability to support changing application requirements over time. However, to effectively enable the sharing of WSN infrastructure amongst various applications over time, security plays a crucial role in controlling interactions between the components that compose applications.

To date, a number of security solutions for WSNs have been proposed in the literature [4], which provide some level of access control by using different authentication schemes comprising of digital signatures, hashing functions, and symmetric or asymmetric keying. However, each of these approaches operate at a coarse-grained level, as they provide a level of entity authentication which considers complete nodes as endpoints. For example, by using these mechanisms, a node is either allowed or disallowed full access to another node. In this work, we envision an access control architecture that provides a more fine-grained level of control where the administrative owner of a node can set policies authorizing access to a particular set of application components or interfaces, rather than to the entire node.

Consider, for example, a custom-made WSN operated by a transport company to monitor temperature inside each of their trailers. Trailers can be picked up by trucks of different companies; when a truck company picks up a trailer, the onboard fleet management system connects to the WSN in the trailer to collect temperature data. The company can access the temperature service, but cannot read product and owner identification data, change alarm thresholds, or activate additional services for humidity, light or vibration sensing.

In this context, we advocate for a per-application access control model in WSNs, which allows the divergent security requirements of co-existing applications to be respected. Our approach is based on a high-level and policy-based way for specifying security. This allows for a clean separation of concerns between, on the one hand, WSN software development and, on the other, WSN administration. Furthermore, support for the dynamic deployment of security policies allows WSN security policies to evolve to meet changing application requirements and regulations.

2. FINE-GRAINED ACCESS CONTROL IN SENSOR NETWORKS

Our approach to realizing fine-grained access control in WSNs is based upon three elements:

- A *loosely-coupled WSN component model*, named LooCI [1], that allows for easy inspection of data flows between the components that compose applications.
- A *flexible and extensible security policy engine*, which allows for fine-grained control of data flows and ensures that these policies can not be circumvented.

*Research for this paper was conducted in the context of the IBBT-DEUS and IWT-SBO-STADiUM projects.

SAC'10 March 22-26, 2010, Sierre, Switzerland.

- A *secure policy distribution channel*, which ensures that only authorized actors may deploy security policies.

The Loosely-coupled Component Infrastructure (LooCI) [1] is a run-time reconfigurable component model following a fully decentralized publish-subscribe interaction model. LooCI components support run-time reconfiguration, interface definitions, introspection, and support for the re-wiring of component bindings. Following this model, applications are implemented as LooCI components that define their provided interfaces as the set of LooCI events they publish, whereas the receptacles of a LooCI component are similarly defined as the events to which they subscribe.

2.1 LooCI Access Control Policy Engine

As illustrated in Figure 1, to control interactions between different application components, a supporting policy framework is deployed on each sensor node consisting of a *Policy Engine* that evaluates all component interactions against a set of policy rules, and a *Secure Policy Distribution* component (discussed in Section 2.2). In this context, we apply flexible access control policies that follow simple Event-Condition-Action (ECA) semantics:

```
policy "allow temperature aggregation" "1" {
   on GET_TEMP as t; //all temperature events
   if( t.src == node_B &&
       t.src_comp == TEMP_AGGREGATION &&
       t.dest_comp == TEMP_SENSOR )
   then( allow t; )
}
```

Listing 1: Example access control policy

Listing 1 illustrates an example access control policy, written by a policy administrator and deployed on node A (see Figure 1). The policy allows all GET_TEMP events to pass between a TEMP_AGGREGATION component on node B and the TEMP_SENSOR component on node A.

Each time an event that is passed between two components is received on the *Event Bus*, the *Policy Engine* evaluates whether it should be allowed to proceed based upon a set of per-node policy rules. If the incoming event matches a policy rule, the associated event (allow or deny) will be applied, whereas the default policy to deal with is deny all. To resolve potential conflicts between multiple matching policies, we follow a priority-based ordering of policies, whereas only the actions of the policy with the highest priority are executed. For more details about the specification of policies and the corresponding framework, we refer to [3].

These policies provide a simple, yet powerful method of controlling access at multiple levels, from *coarse*-grained node-level access control used to control all interactions between nodes, *fine*-grained component-level access control to govern interactions between two components, and *super-fine*-grained interface-level access control used to control very specific interactions between component interfaces. Furthermore, we provide tool support for policy administrators, allowing them to easily select which nodes, components or interfaces they wish to apply access control policies to.

2.2 Secure Policy Deployment

As access control policies provide control over all aspects of component interaction on the network, it is particularly critical that these policies are disseminated in a secure fashion. Hence, policy distribution is performed over a dedicated

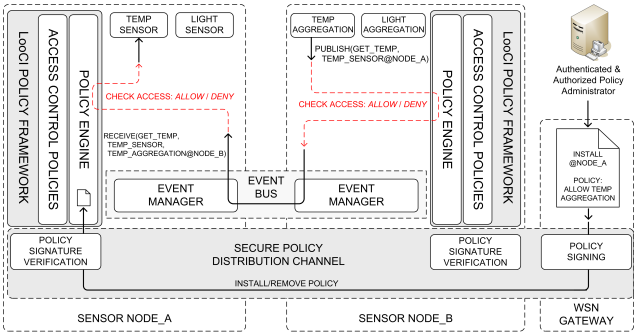

Figure 1: The LooCI Policy Framework

security bus between the authorized policy administrator back-end, the WSN gateway, and each sensor node.

To deploy a policy on a particular sensor node, a secure connection between the policy administrator back-end and WSN gateway is set up using standard enterprise-grade security technologies such as TLS/SSL over which the digitally signed policy is transferred. Secondly, the WSN gateway verifies the identity of the policy administrator, the integrity of the received policy, and it checks whether the administrator is allowed perform this management action. Finally, if allowed, the policy is safely distributed to the sensor node using one of the standard WSN security solutions [4].

As this distribution architecture provides support for dynamic deployment of new policies, the framework can be adapted according to evolving application demands over time.

3. STATUS AND FUTURE WORK

We have realized and evaluated [3] an initial implementation of the proposed architecture for the Sun SPOT [5] sensor node platform. This implementation addresses the concerns of providing flexible and fine-grained security support while respecting the resource-constrained nature of WSNs in terms of memory footprint and performance overhead.

Future work will focus upon three key fronts (i.) extending our security architecture to consider more complex application scenarios, (ii.) real world user trials in a logistics scenario [2], and (iii.) expansion of our policy language to support the enforcement of more security operations such as selective encryption of data flows between two components.

4. REFERENCES

[1] D. Hughes, K. Thoelen, W. Horré, N. Matthys, J. Del Cid, S. Michiels, C. Huygens, and W. Joosen. LooCI: a loosely-coupled component infrastructure for networked embedded systems. In *Proceedings of MoMM'09*, New York, NY, USA, Dec. 2009. ACM.

[2] IWT STADiUM project 80037. Software technology for adaptable distributed middleware.

[3] N. Matthys, D. Hughes, S. Michiels, C. Huygens, and W. Joosen. Fine-grained tailoring of component behaviour for embedded systems. In *The 7th IFIP Workshop on Software Technologies for Future Embedded and Ubiquitous Systems*, November 2009.

[4] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: security protocols for sensor networks. *Wirel. Netw.*, 8(5):521–534, 2002.

[5] Sun SPOT World. http://www.sunspotworld.com/.